# Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 07 August 2003

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

## Daily Overview

- Dow Jones Business News reports that a Romanian Web site that for weeks had been displaying stolen credit−card numbers and other private information belonging to more than 450 people, mostly residents of the U.S., was taken offline Wednesday. (See item 6)
- According to the Minneapolis Star Tribune, the U.S. Department of Agriculture (USDA) said Tuesday that Ellison Meat Company of Pipestone, MN, is voluntarily recalling about 194,700 pounds of frozen ground beef products that might be contaminated with E. coli O157:H7 bacteria. (See item 15)
- The Washington Post reports Del. Eleanor Holmes Norton, a member of the Select Committee on Homeland Security, called yesterday for a congressional hearing on whether the sale of fake identification cards in Adams Morgan and other parts of the country could attract terrorists. (See item 20)

**DHS/IAIP Update *Fast Jump***

**Production Industries:** Energy; Chemical; Defense Industrial Base
**Service Industries:** Banking and Finance; Transportation; Postal and Shipping
**Sustenance and Health:** Agriculture; Food; Water; Public Health
**Federal and State:** Government; Emergency Services
**IT and Cyber:** Information and Telecommunications; Internet Alert Dashboard
**Other:** General; DHS/IAIP Web Information

## Energy Sector

**Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated**
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *August 06, The Associated Press* — **U.S. pumping oil into strategic reserves.** The Department of Energy (DOE) has been purchasing oil for the Strategic Petroleum Reserve (SPR), and while there is debate about its impact on the commercial price of gasoline, DOE spokesman Joe Davis

said **both Democrats and Republicans in Congress have made clear they want the strategic reserve, now at 611 million barrels, filled to its 700−million−barrel−capacity.** Commercial U.S. oil stocks have been at uncomfortable levels all year, putting upward pressure on prices. A number of analysts said the supply problem stems from a variety of factors: the problem in getting Iraqi oil flowing again; OPEC producers carefully scrutinizing production; and U.S. refiners refusing to buy oil at $30 or more when they anticipate lower prices. **Since January 2002, the amount of oil in the SPR has increased from 554 million barrels to nearly 611 million. The United States uses about 20 million barrels of oil a day, with about half coming from imports.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A22302−2003Aug 6.html

2. *August 06, Chicago Tribune* — **Nuclear power may get second chance with first new reactor in decades. The owners of a once−troubled nuclear power plant in Clinton, IL, are preparing to file for permits to build another one nearby, perhaps the nation's first new reactor since the 1970s.** After the partial meltdown at Three Mile Island in 1979, the industry essentially stopped ordering new plants. But this fall, three utilities are expected to apply for "early site permits" to reserve spots for the next generation of nuclear reactors. A reply to the permit could take up to two years, and any final decision on whether to build in Clinton or at the other sites could be years away. An early site permit secures land, consolidates the cumbersome approval process and gives a company at least 20 years to decide whether to build a plant. It does not, however, have to commit to construction or specify the reactor type. Often derided as too costly, inefficient and financially risky, the nuclear industry has been helped by consolidation, deregulation in some markets and the simplification of labyrinthine government regulations. **Heartened by the new regulatory process and by the economic potential of their units, approximately half of the 103 U.S. operating plants have applied for 40−year license renewals and more are expected, according to the Nuclear Energy Institute.**
Source: http://www.centredaily.com/mld/centredaily/news/6470033.htm

3. *August 05, Chattanoogan.com* — **Missing weapon found at Sequoyah nuclear plant. An automatic weapon that has been missing at the Sequoyah Nuclear Plant since July 1 was found on Monday, August 4.** A Tennessee Valley Authority (TVA) spokesperson said the weapon was supposed to be kept in a storage location for use by the provider of security services at the plant, Pinkerton Government Services. TVA Police are investigating the incident and are cooperating with nuclear security.
Source: http://www.chattanoogan.com/articles/article_39471.asp

[Return to top]

## Chemical Sector

Nothing to report.
[Return to top]

## Defense Industrial Base Sector

4.

*August 05, Federal Computer Week* — **Military must reshape R&D.** At a recent research and development (R&D) conference, Retired Navy Vice Admiral Arthur Cebrowski, director of DoD's Force Transformation Office, stated that **the way wars are fought is changing, and the R&D community has to change with it.** He added that all elements of war−−from fires to intelligence to logistics−−must be reworked to reflect an Information Age when joint systems and instant access to data are critical, and that command, control and communications capabilities should be built with joint interdependency in mind, not interoperability. Cebrowski continued to state that **the military should focus on four risk management areas: people; joint science and technology projects and funding; joint experimentation; and tools for modeling a complete battlefield picture that shows how forces interact.**
Source: http://www.fcw.com/fcw/articles/2003/0804/web−navy−08−05−03. asp

5. *August 05, American Forces Press Service* — **DoD will examine options before requesting more troops. Before the Department of Defense (DoD) asks congress to authorize more soldiers, the department would like to see if there are other ways to handle deployments without raising the troop ceiling, Defense Secretary Donald H. Rumsfeld said during a Pentagon news conference on Tuesday, August 5.** Rumsfeld listed a number of options. The military can put in place a more efficient deployment and redeployment process. The services also should examine−−as the Navy is−−using technology to cut down manning necessary for ships and other weapons systems. He said the services must look at "rebalancing the reserve component with the active force component so that we don't have to have the kinds of call−ups that we do now." Another option is to take the 300,000 to 380,000 U.S. military members who are in jobs better done by civilians and return them to military roles. Rumsfeld wants to make the most effective use of the force.
Source: http://www.defenselink.mil/news/Aug2003/n08052003_200308055. html

[Return to top]

## Banking and Finance Sector

6. *August 06, Dow Jones Business News* — **Romanian web site displaying consumers' data shut down. A Romanian Web site that for weeks was displaying stolen credit−card numbers and other private information belonging to more than 450 people, mostly residents of the U.S., was taken offline Wednesday**. The site apparently served as an online meeting place for a handful of hackers. Two members, one using the handle "Light" and another using " aolongvuong," each deposited card lists on the site in mid− to late−June. All 13 of the site's members, who aren't necessarily Romanian, joined and posted comments during June and July in various areas of the site, some of which provide hacker programs. **The lists, which contained the addresses, phone numbers and e−mail addresses of holders of Discover, Visa, MasterCard and American Express cards, were long exposed to the elements, although at least two of the major credit−card companies said they asked the company hosting the site, MobiFon, to shut it down.** A MobiFon spokesperson said the company would comply within 24 hours of the complaint if it wasn't able to reach the site owner, or sometime Wednesday, she said.
Source: http://biz.yahoo.com/djus/030806/1344001204_1.html

7.

*August 04, Computerworld* — **Encryption mandate puts strain on financial IT. A mandate by credit card companies and related funds−transfer networks to upgrade the security of electronic transactions will cost the banking and retail industries billions of dollars in hardware and software and require several years of intensive work to complete.** MasterCard International Inc., Visa U.S.A. Inc. and associated network providers have established deadlines starting in 2004 for converting electronic funds networks to the Triple Data Encryption Standard (DES). The DES cryptology algorithm currently in use has become vulnerable to attacks as a result of increases in computing power, those organizations say. In addition to being more secure, the new machines may be Web−enabled and ready to support a host of new features such as online bill payment, account aggregation and brokerage services. **DES is designed to protect personal identification numbers entered at ATMs and point−of−sale devices, but using brute−force computing power in a process called an "exhaustion attack," it's possible to unscramble DES−protected information.** A new ATM can cost as much as $50,000; costs will range from $1,000 to $5,000 for ATMs that can be upgraded, according to financial industry analysts.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,83685,00.html

[Return to top]

## Transportation Sector

8. *August 06, Associated Press* — **Longer lines expected at airports in wake of advisory. Travelers may encounter longer lines at airports as screeners focus extra attention on CD players, cameras, laptops and other electronic gadgets that terrorists might try to use to conceal weapons or bombs.** The Department of Homeland Security sent an advisory on Tuesday to law enforcement personnel nationwide alerting them to the possibility al Qaeda could use electronics to carry out attacks. **"Al Qaeda operatives have shown a special interest in converting a camera flash attachment into a stun gun type of weapon or improvised explosive device," the advisory said. David Stempler, president of the Air Travelers Association, said longer lines will be a small price to pay for extra security.** "There's one thing worse than being slightly inconvenienced −− it's being permanently inconvenienced," he said. Ian Redhead, spokesman for the airport trade group Airports Council International, said the more intense scrutiny of electronics may at first lead to longer lines. But, he said, airports wouldn't put up with waits that last more than 10 minutes, the standard the government has set for its screeners.
Source: http://www.cnn.com/2003/TRAVEL/08/06/aviation.security.ap/in dex.html

9. *August 06, Associated Press* — **Delays, congestion clog Midway.** Located just 10 miles from Chicago's Loop, Midway Airport has a reputation as a small gem of an airport where travelers can escape the long lines and parking hassles of O'Hare. **But security procedures put in place after the terrorist attacks of September 11, 2001, an increase in passengers and a bottleneck−prone layout are resulting in chronic delays.** Speaking a day after travelers waited up to an hour in a line leading to the airport's 10 security lanes and four airlines were forced to hold flights, Mayor Richard Daley said federal officials need to hire more screeners. **Midway is in the midst of an $800 million overhaul that will add 12 aircraft gates to the current 31, but since the redesign was planned before the terrorist attacks, it will do little to alleviate the security delays.** There is only one security checkpoint at the airport, and it

leads to 10 security lanes. Other than an 11th security lane being added this weekend, there is no space for more screeners, according to the Transportation Security Administration, which is in charge of airport security.
Source: http://www.indystar.com/print/articles/3/063305−1143−031.htm l

10. *August 06, Associated Press* — **Boating officials fine−tuning rules.** Watermark Cruises (Annapolis, MD) owner Debbie Gosselin recently told Coast Guard officials that requiring commercial boats to carry expensive, but questionable, security equipment could destroy the local maritime community. **As proposed, the Maritime Transportation Security Act of 2002 aims to boost security at U.S. coastal facilities, ports and ships by July 2004. But many fear it could affect charter boat companies and operators, perhaps even driving smaller companies out of business.** The Department of Homeland Security on July 1 released interim rules that require 10,000 ships, 5,000 coastal facilities and the nation's 361 ports to draft and implement security plans. The Coast Guard says ports, ships, coastal facilities and offshore oil drilling units will have to spend $7.3 billion over the next 10 years on equipment, personnel and training. **Under the rules, people waiting to board large passenger ships, including ferries, could be subject to the types of body and baggage screening now in place at airports. But a Coast Guard official said that would happen only during times when the nation's terror alert has been raised to orange, for "high," and only on certain ships deemed most vulnerable.**
Source: http://www.hometownannapolis.com/cgi−bin/read/2003/08_05−17/ BUS

11. *August 06, Associated Press* — **Coast Guard issues terrors warning to ferry companies.** The U.S. Coast Guard has issued a warning to ferries that carry commuters into the city to be on the lookout for terrorists. **The Coast Guard cited "suspicious activity" and "possible surveillance of ferry operations around the U.S. over the past few months," and encouraged ferry operators to be aware of items ranging from unattended briefcases to pier−side observers.** Authorities did not identify any specific targets, but described ferries as "soft targets" because of the minimal checks done to determine whether explosives have been carried onto the vessel, the Daily News reported Wednesday. **The warning also said that the boats could be commandeered or used as a weapon against other ferries.** Spokespeople for the Staten Island Ferry and NY Waterway said they have encouraged their employees to be vigilant, the paper said.
Source: http://www.newsday.com/news/local/wire/ny−bc−ny−−attacks−fer ries0806aug06,0,572770.story?coll=ny−ap−regional−wire

12. *August 05, Todays Trucking* — **CTA working FAST for trucker security card.** After receiving positive feedback from the Canadian government last month, **the Canadian Trucking Alliance (CTA) said that U.S. authorities are also warming to the idea of allowing the FAST card to be used as an all−purpose security I.D. for Canadian truckers.** Asa Hutchinson, Under Secretary of Border & Transportation Security at the U.S. Department of Homeland Security, said he likes the CTA's suggestion that the Free and Secure Trade (FAST) card process be used for security credentialing of Canadian truck drivers. **The CTA has been concerned with the ability of Canadians to comply with new U.S. hazmat requirements and to obtain a U.S. Transportation Worker Identity Card (TWIC), which will be required by all U.S. transportation workers in the near future, but for which there is presently no mechanism for Canadian truck drivers to even apply for.**

Source: http://www.todaystrucking.com/displayarticle.cfm?ID=2595

[Return to top]

## Postal and Shipping Sector

Nothing to report.
[Return to top]

## Agriculture Sector

13. *August 05, Wisconsin Ag Connection* — **New Mexico's TB status downgraded. The U.S. Department of Agriculture's (USDA) Animal Plant Health Inspection Service (APHIS) has downgraded the bovine tubeculosis (TB) status of the state of New Mexico from an accredited−free state to a modified accredited advanced state**. APHIS's change, effective July 24, means that **dairy cattle can only move directly to an approved slaughtering establishment or move interstate from New Mexico from an accredited herd certified accredited within one year of movement, or be officially identified and move on a negative official tuberculin test conducted within 60 days prior to the date of movement.** Recently, two TB−affected dairy herds were detected in Roosevelt County. Under current USDA regulations, if two or more affected herds are detected in an accredited−free state or zone within a 48−month period, the state or zone will be removed from the list of accredited−free areas, and will be reclassified as modified accredited advanced.
Source: http://www.wisconsinagconnection.com/story−national.cfm?Id=8 41&yr=2003

14. *August 05, AgWeb* — **Permits for industrial biotech plants. U.S. Department of Agricultures's (USDA) Animal and Plant Health Inspection Service (APHIS) is amending its biotechnology regulations as they pertain to plants designed to produce industrial compounds. Entities wishing to move, field test or import these types of engineered plants must apply for a permit**. Previously, APHIS allowed companies and institutions to field test, move, or import plants genetically engineered to produce industrial compounds under its notification process, which is an expedited permitting procedure. The notification process was originally added to the biotechnology regulations in order to expedite introductions for genetically engineered plants considered low risk and developed using genetic modifications with which APHIS was already familiar. Recently, requests involving genetically engineered industrial plants have utilized new, less familiar processes and non−food, non−feed traits that no longer qualify for the notification process. **This interim rule strengthens APHIS regulations for field testing of genetically engineered industrial plants in anticipation of an increase in requests regarding these types of plants**.
Source: http://www.agweb.com/news_show_news_article.asp?file=AgNewsArticle_2003851513_1412&articleid=100052&newscat=WA

[Return to top]

## Food Sector

15. *August 06, Minneapolis Star Tribune* — **Meatpacker recalls possibly contaminated beef. Ellison Meat Company of Pipestone, MN, is voluntarily recalling about 194,700 pounds of frozen ground beef products that might be contaminated with E. coli O157:H7 bacteria, the U.S. Department of Agriculture (USDA) said Tuesday.** The recall was initiated because preliminary investigations suggest that the ground beef might be linked to two Colorado people who were sickened by E. coli, the USDA said. The recalled products were sold to restaurants and through door−to−door sales nationwide. The meat was processed between May 30 and June 11. "All of the restaurants and all of the distributors have been notified," said Alan Sheldon, spokesman for Ellison, also known as Howard Beef Processors. E. coli O157:H7 is a potentially deadly bacteria that can cause diarrhea and dehydration.
Source: http://www.startribune.com/stories/1405/4026941.html

16. *August 05, Federal Computer Week* — **FDA seeks food illness model. The Food and Drug Administration (FDA) plans to create a modeling tool for food threats. FDA officials want a simulation that can predict the outcome and determine possible causes of food contamination outbreaks, based on variables such as illness symptoms and characteristics of a public health response. Officials could then simulate responses.** "This system should be able to model the flow of food but also let us manipulate variables to create what−if scenarios," said Morris Potter, the FDA's project officer. The tool would outline where to find and how to extract data, such as food production and distribution, human consumption patterns, and illness symptoms and outcomes. "It helps us predict what happens when certain things go wrong so we can be better prepared, and it helps us prioritize," Potter said. Officials also expect to be able to run the system in reverse, entering outcomes to predict the origin. **Once agency officials award a contract, they expect to have a basic model within a year.**
Source: http://www.fcw.com/fcw/articles/2003/0804/web−fda−08−05−03.a sp

[Return to top]

## Water Sector

Nothing to report.
[Return to top]

## Public Health Sector

17. *August 06, Orlando Sentinel* — **U.S. responds poorly to animal−borne ills. The U.S. is unprepared to deal with animal−borne infections.** A report issued Tuesday said health agencies trip over one another while reacting to the latest crisis, yet do little to prevent animal diseases from spreading to people in the first place. The group looked at how U.S. officials are handling five illnesses that started in animals: monkeypox, West Nile virus, mad−cow disease, Lyme disease, and chronic wasting disease. In each instance, the report identified serious obstacles in timely identification of the disease and the government's ability to contain an outbreak. Shelley Hearne, a public−health scholar at Johns Hopkins University, said **it's pure luck that recent animal−borne infections haven't grown into massive epidemics. The report cites the sheer number of agencies involved in animal−borne diseases as one stumbling block.** For example, state and local agencies, four Cabinet−level departments, and

five federal agencies were called into action for the recent monkeypox scare. The report said, **the danger of animal−borne infections will increase because people are moving into previously uninhabited regions of the world, and with today's plane−traveling society, one person with an animal−borne infection can transport the disease quickly.**
Source: http://www.orlandosentinel.com/news/custom/science/orl−asecanimals06080603aug06,0,4203620.story?coll=orl−news−headlines

18. *August 05, Scientist* — **New Health Protection Agency defines its priorities. The new UK public health organization, the Health Protection Agency (HPA), Tuesday set itself a wide range of priorities for the next five years.** The agency outlined 12 strategic goals, ranging from boosting preparedness for emergencies to better understanding of the effects of chronic exposure to environmental chemicals and radiation. **Among the first priorities will be establishing a more systematic approach to "horizon scanning" for anticipating problems**, the agency's Chief Executive Pat Troop said. **Developing better communication systems to identify and track exposures to infection, chemicals, and radiological hazards is also an important goal**, she said. The early results of modeling the spread of some vectors should be completed by the end of the year, she said. **The HPA also wants to strengthen preparations for a quick response to health emergencies by developing specific countermeasures and training staff in their implementation.** "There is a whole raft of new work we are embarking on, from establishing a network of local health protection teams around England, through to taking international collaboration to another level," Troop said.
Source: http://www.biomedcentral.com/news/20030805/02

19. *August 05, New York Times* — **China lags in sharing SARS information. China's crash research program into Severe Acute Respiratory Syndrome (SARS) has yielded important new clues. But little of that information has been widely shared, dismaying World Health Organization (WHO) officials, who worry that opportunities to prevent a possible return of the disease in the fall could be missed.** In May, the Chinese government put SARS research on a fast track and invested millions of dollars in 95 projects. While much of the Chinese research is first−rate, the WHO's Dr. Stöhr said, "many groups are working on SARS, but do not know what the others are doing except by reading Chinese newspaper accounts, and many accounts do not provide the necessary scientific information." China had more than 3,000 cases of SARS, the most reported anywhere, and was probably the point of origin for the epidemic last year. Given that experience, China could yield significant research for its own public health officials and for the rest of the world.
Source: http://www.nytimes.com/2003/08/05/health/05SARS.html

[Return to top]

## Government Sector

20. *August 06, Washington Post* — **Norton calls ID markets terror magnet. Del. Eleanor Holmes Norton (D−DC), a member of the Select Committee on Homeland Security, called yesterday for a congressional hearing on whether the sale of fake identification cards in Adams Morgan and other parts of the country could attract terrorists**. U.S. immigration authorities have cracked down recently on the notorious market along Columbia Road NW in DC, where vendors for years have peddled fake Social Security cards, U.S. residency permits

and other documents. On a national level, meanwhile, **immigration officials have been so overwhelmed by new anti−terrorism tasks that they have reduced the number of investigations into fake document rings**, officials from the Bureau of Immigration and Customs Enforcement said. They said most purchasers of the fake cards were unauthorized immigrants hoping to use them to get jobs. Norton emphasized that she didn't think such immigrants were terrorists, but said she is worried that the easy availability of phony IDs could be exploited.
Source: http://www.washingtonpost.com/wp−dyn/articles/A22005−2003Aug 5.html

**21.** *August 06, Washington Post* — **Crossing lines to fight terrorism.** Authorities in the District and four large Eastern states plan to launch an anti−terrorism data−sharing effort in September to enable federal, state and local agencies to search instantly through millions of law enforcement records, Mayor Anthony A. Williams said yesterday. **Virginia, Maryland, Pennsylvania and New York have been invited to join the District's $4 million, Internet−based Justice Information System, underscoring counter−terrorism cooperation among jurisdictions most affected by the September 11, 2001, attacks, District officials said.** Williams (D), meeting with U.S. Homeland Security Secretary Tom Ridge, Maryland Lt. Gov. Michael S. Steele (R) and Virginia security chief John H. Hager on the anniversary of a summit to discuss regional emergency preparedness, said the 911 Connection project was developed with federal support. **Williams said the pilot program would share criminal justice information, "not only for emergency preparedness, but for regular, garden−variety crime−fighting." "One of the most important things we can do as a [national capital] region is to access common information," said Ridge, who praised the initiative.** "This pilot program is to give most of the jurisdictions access to that information."
Source: http://www.washingtonpost.com/wp−dyn/articles/A21710−2003Aug 5.html

[Return to top]

## Emergency Services Sector

**22.** *August 06, Oakland Tribune Online* — **County gets $3.4 million to fight terror.** California Gov. Gray Davis trumpeted allocation of $119 million in federal homeland security funds Monday to state and local public safety agencies, but agreed with Bay Area officials the funding flow is inadequate−−especially amid the latest terrorism warnings. **About four−fifths of the money will be awarded to county and city agencies statewide for joint training and equipment purchases,** with $3.4 million going to Alameda County, nearly $2.3 million to Contra Costa County, about $1.65 million to San Mateo County and more than $1.4 million to San Joaquin County. In addition, Davis announced the allocation of nearly $16 million to reimburse local agencies throughout California for personnel overtime costs during the Iraq war when there was a higher terror alert. **Of the roughly $20 million that will be allocated to statewide agencies, the bulk of the funds will go to the California Highway Patrol, National Guard and California Department of Forestry and Fire Protection.** California's state and local agencies have spent more than $700 million on homeland security since the September 11, 2001 terrorist attacks on the East Coast and have only received about $500 million in federal funding, state officials said.
Source: http://www.oaklandtribune.com/Stories/0,1413,82~1726~1555354 ,00.html

**23.** *August 05, Associated Press* — **State, federal anti−terrorism efforts combine in Alaska. Separate state and federal anti−terrorism task forces in Alaska have merged into a single new group. Officials say the merger should allow them to work more efficiently.** Alaska's U.S. Attorney Timothy Burgess said he believes Alaska is the first state to combine state and federal homeland security task forces. It makes sense here because of the limited resources available to cover a large geographical area, he said. **The new Anti−terrorism Task Force of Alaska replaces the Governor's Homeland Security Task Force and the federal Anti−terrorism Task Force for Alaska.** Some of the same people were on both groups, so joining forces will cut down on the number of meetings they have to attend, eliminate some duplication of effort and prevent tasks from being overlooked, Burgess said. Department of Military and Veterans Affairs Commissioner Craig Campbell is co−chairman of the new task force group along with Burgess. **About 60 agencies and offices are represented on the task force. They include federal and state law enforcement agencies, local governments and private businesses involved in fields such as transportation and communications. All branches of the military are also participating.**
Source: http://www.peninsulaclarion.com/stories/080503/ala_080503ala.003001.shtml

[Return to top]

## Information and Telecommunications Sector

**24.** *August 06, Wired* — **Forums point the way to Jihad.** With the Taliban out of Afghanistan and governments around the world restricting access to al Qaeda−linked websites, would−be militant Islamic holy warriors are turning to low−tech electronic message boards to find out where to fight. **The message boards, hosted by such domains as Yahoo and Lycos in the UK, are proving a free, unrestricted and largely difficult−to−track forum for would−be fighters to hook up with those coordinating operations**, say terrorism experts and intelligence officials. Whereas once Islamic militants needed to pass through training camps in Afghanistan to be groomed for jihad, now **they are announcing their desire to fight in Muslim holy wars and martyr attacks from cybercafes and home computers in Malaysia, Pakistan, Saudi Arabia and the UK**.
Source: http://www.wired.com/news/culture/0,1284,59897,00.html

**25.** *August 06, Government Computer News* — **Wireless network attacks get a public airing. Federal grants are funding research by investigators in the computer science departments of the nation's universities to probe the vulnerabilities of wired and wireless networks**. Some of the results of that research were presented Wednesday at the Security Symposium in Washington sponsored by the USENIX Association of Berkeley, CA. A team from Stanford University, in one example, used a timing attack to extract a private encryption key from a server across a network. In another, researchers at the University of California at San Diego perfected denial−of−service attacks against 802.11 wireless networks. Both teams also demonstrated how to defend against the attacks.
Source: http://www.gcn.com/vol1_no1/daily−updates/23053−1.html

**26.** *August 05, ComputerWeekly* — **Companies' poor security policies hamper police investigations into computer crime. Police forces in the UK are having to abandon investigations into computer crimes committed by employees at work because employers**

**are failing to enforce their security policies**, a senior detective revealed last week. Steve Santorelli, detective sergeant at Scotland Yard's Computer Crime Unit, said a significant percentage of police investigations fail to get off the ground because employers have not spelt out to staff what is and is not acceptable. Cases where employees copy sensitive data by gaining unauthorized access to their employers' systems, or change the contents of web pages without permission, can be difficult to prosecute unless companies clearly lay down the boundaries. **Many security policies do not warn staff of the dangers of social engineering attacks from hackers looking to bypass security systems by conning people in to revealing important company information that will allow the hackers to access systems**.
Source: http://www.computerweekly.com/articles/article.asp?liArticle ID=123928

### Internet Alert Dashboard

**Current Alert Levels**

| | |
|---|---|
| AlertCon: 1 out of 4<br>https://gtoc.iss.net | Security Focus ThreatCon: 2 out of 4<br>http://analyzer.securityfocus.com/ |

**Current Virus and Port Attacks**

| | |
|---|---|
| **Virus:** | #1 Virus in the United States: **JS_CBASE.EXP1**<br>Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center<br>[Infected Computers, North America, Past 24 hours, #1 in United States] |
| **Top 10 Target Ports** | 445 (microsoft−ds), 80 (www), 137 (netbios−ns), 1434 (ms−sql−m), 139 (netbios−ssn), 113 (ident), 0 (−−−), 25 (smtp), 135 (epmap), 53 (domain)<br>Source: http://isc.incidents.org/top10.html; Internet Storm Center |

[Return to top]

## General Sector

27. *August 06, Washington Post* — **U.S. to file terrorism charges against Pakistani detainee. Federal authorities expect to file terrorism charges soon against a detained Pakistani man with ties to the shipping industry and links to a senior al Qaeda leader**, law enforcement officials said Tuesday. Uzair Paracha, 23, has been secretly detained as a material witness since his arrest March 31 in the offices of a New York clothing import firm owned by his father, sources said. **Authorities believe the Paracha family business may have been used as cover for attempts to smuggle al Qaeda operatives or weapons into the United States**. Paracha's father, who owns a Pakistani textile company that routinely shipped large containers of clothing and other goods into Newark, was last seen as he tried to board an airplane in Karachi a month ago. He was arrested by Pakistani police and has been held incommunicado ever since, according to local press reports and two U.S. officials with knowledge of the case. **U.S. officials first obtained the information that led to Paracha's arrest from Khalid Sheik**

**Mohammed, the senior al Qaeda lieutenant who masterminded the September 11, 2001, attacks** and who was arrested by U.S. forces earlier the same month, two sources said.
Source: http://www.washingtonpost.com/ac2/wp−dyn/admin/emailfriend?contentId=A21659−2003Aug5&sent=no

28. *August 06, The Associated Press* — **U.S. finds cache in series of Iraq raids. U.S. forces said Wednesday they arrested 19 suspected members of the anti−U.S. resistance and killed another, and found a huge stockpile of weapons in a series of raids in northern Iraq**. The U.S. military said Iraqi police officers arrested a man who was organizing guerrilla attacks against American soldiers Sunday. Eighteen other suspected guerrillas were arrested in seven overnight raids across north−central Iraq, Major Josslyn Aberle said. She also said soldiers uncovered a large weapons cache 25 miles northeast of Tikrit, Saddam's hometown, on Sunday.
Source: http://abcnews.go.com/wire/World/ap20030806_838.html

29. *August 05, U.S. Department of State* — **Public Announcement: Laos.** At least three bomb attacks over the past several weeks targeting buses and bus stations in Vientiane and southern Laos have resulted in death and injury to passengers. We have also received reports of small−scale attacks by anti−government groups in isolated areas along the Lao−Thai border. **The Department of State cautions U.S. citizens that there have been renewed attacks on all forms of transportation in Laos**, especially along Route 13, the main road from Vang Vieng to Luang Phrabang. In light of these attacks **we recommend that American citizens avoid travel by road between Vang Vieng and Luang Phrabang. We also recommend that travelers avoid travel or activities in the surrounding areas of Vang Vieng**. U.S. citizens residing in or traveling to Laos are encouraged to register at the Consular Section of the U.S. Embassy in Vientiane and enroll in the warden system (emergency alert network) to obtain updated information on travel and security in Laos. This Public Announcement expires on February 5, 2004.
Source: http://travel.state.gov/laos_announce.html

30. *August 05, USA Today* — **Threat of terrorism poses special challenge to hotels. The car bomb explosion Tuesday at the 2−year−old JW Marriott in Jakarta, Indonesia, underscores the difficulty the hospitality industry faces in appearing inviting to travelers but forbidding to terrorists**. The Indonesian attack was the third in just over a year at upscale foreign franchises of U.S. hotel chains, including a suicide bombing outside the Marriott hotel in Karachi in June 2002 and a suicide bombing outside a Sheraton property in Karachi in May 2002. Recognizing security as a requirement for international travelers, **most large hotels in Asia and the Middle East employ extensive security, often including armed guards and bomb−resistant glass. In addition, a new federal law providing government financial support for anti−terrorism insurance is about to take effect**. The measure is expected to give builders and insurers the assurance they have asked for before starting construction of high−profile properties.
Source: http://www.usatoday.com/money/biztravel/2003−08−05−hotels_x. htm

[Return to top]

## DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

### DHS/IAIP Daily Open Source Infrastructure Report Contact Information

| | |
|---|---|
| Content and Suggestions: | nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 |
| Subscription and Distribution Information | Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−6631 for more information. |

### Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

### DHS/IAIP Disclaimer